



(12) **United States Patent**
Bauer et al.

(10) **Patent No.:** **US 8,417,947 B2**
(45) **Date of Patent:** ***Apr. 9, 2013**

(54) **ELECTRONIC AUTHORIZATION SYSTEM AND METHOD**

(75) Inventors: **Stephanie Bauer**, Arlington, VA (US); **Jonathan N. Freedman**, Chevy Chase, MD (US); **Daniel J. Lane**, North Potomac, MD (US); **Miriam Jaffe**, Columbia, MD (US); **Susan M. Zloth**, Castle Rock, CO (US)

(73) Assignee: **Merchant Link, LLC**, Silver Spring, MD (US)

(*) Notice: Subject to any disclaimer, the term of this patent is extended or adjusted under 35 U.S.C. 154(b) by 0 days.

This patent is subject to a terminal disclaimer.

(21) Appl. No.: **13/221,719**

(22) Filed: **Aug. 30, 2011**

(65) **Prior Publication Data**

US 2011/0314277 A1 Dec. 22, 2011

Related U.S. Application Data

(60) Continuation of application No. 11/366,189, filed on Mar. 2, 2006, now Pat. No. 7,451,481, and a division of application No. 12/250,336, filed on Oct. 13, 2008, now Pat. No. 8,010, 791.

(60) Provisional application No. 60/676,681, filed on Apr. 29, 2005.

(51) **Int. Cl.**
H04L 29/06 (2006.01)

(52) **U.S. Cl.** **713/167; 705/64; 705/75**

(58) **Field of Classification Search** None
See application file for complete search history.

(56) **References Cited**

U.S. PATENT DOCUMENTS

5,978,918	A	11/1999	Scholnick et al.
6,332,193	B1	12/2001	Glass et al.
6,938,019	B1	8/2005	Uzo
6,938,022	B1	8/2005	Singhal
6,990,470	B2	1/2006	Hogan et al.
7,082,415	B1	7/2006	Robinson et al.

(Continued)

OTHER PUBLICATIONS

Shift4 Releases New Technology to Insure the Security of its Merchants' and Partners' Payment Processing, Tokenization Moves the Liability for Securing Credit Card Data Away from Merchants' and POS Application Developers, Las Vegas, Nevada, Oct. 5, 2005, 2 pgs.
Mark, Heather, Storing Credit Card Data, A Look at the Business Needs, Regulations and Solutions Surrounding the Issue, CISSP, Jan. 2006, 44 pgs.

(Continued)

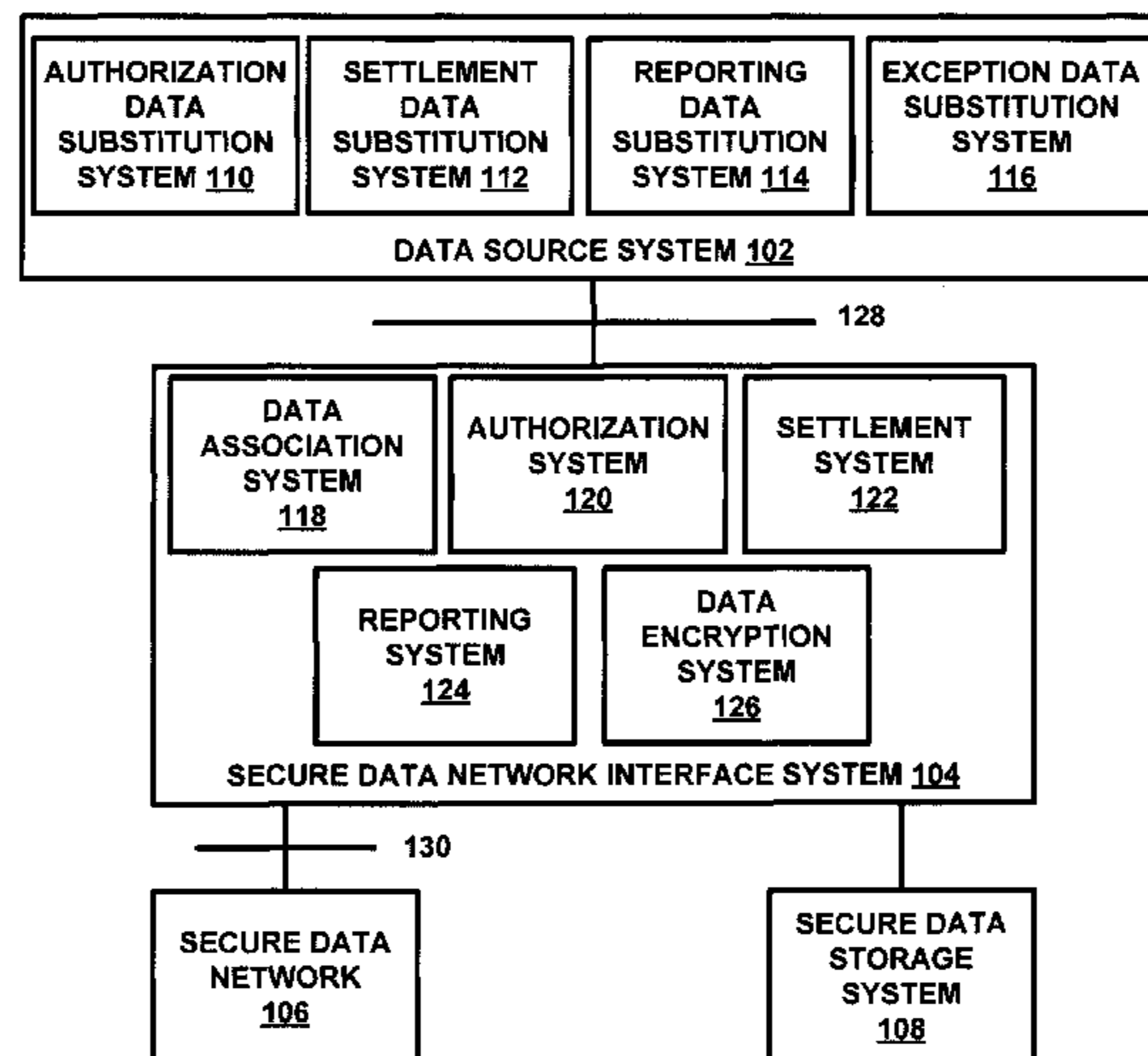
Primary Examiner — David Pearson

(74) *Attorney, Agent, or Firm* — Jackson Walker L.L.P.; Christopher J. Rourk

(57) **ABSTRACT**

An electronic authorization system comprising a data source system configured to transmit transaction data. A secure data system is coupled to the data source system over an open network, the secure data system is configured to receive the transaction data from the data source system, generate a unique encrypted identifier for the transaction data and to transmit the unique encrypted identifier to the data source system. The data source system is configured to receive the unique encrypted identifier and replace payment card data associated with the transaction data in a database with the unique encrypted identifier.

19 Claims, 2 Drawing Sheets



U.S. PATENT DOCUMENTS

7,376,629 B1 5/2008 McIsaac et al.
7,512,236 B1 3/2009 Zhu
2002/0007320 A1 1/2002 Hogan et al.
2002/0022967 A1 2/2002 Ohkado
2002/0133467 A1 9/2002 Hobson et al.
2002/0191020 A1 12/2002 Kaply et al.
2003/0046237 A1 3/2003 Uberti
2003/0061171 A1 3/2003 Gilbert et al.
2004/0073668 A1 4/2004 Bhat et al.
2004/0172309 A1 9/2004 Selwanes et al.
2004/0210449 A1 10/2004 Breck et al.
2005/0198111 A1* 9/2005 Lamb et al. 709/203

OTHER PUBLICATIONS

Letter from Michael J. Andelson of Best Best & Krieger LLP to Christopher Justice, President, Merchant Link, LLC and Michael P. Duffy, Chief Executive Officer of Chase Paymentech Solutions, LLC, dated Dec. 14, 2006, 4 pgs.
United States Patent and Trademark Office, International Search Report and Written Opinion, PCT Application No. PCT/US2006/016745, Jun. 18, 2007, 8 pgs.
Canadian Patent Office, Office Action, Patent Application No. 2,606,183, Jan. 28, 2011, 4 pgs.

* cited by examiner

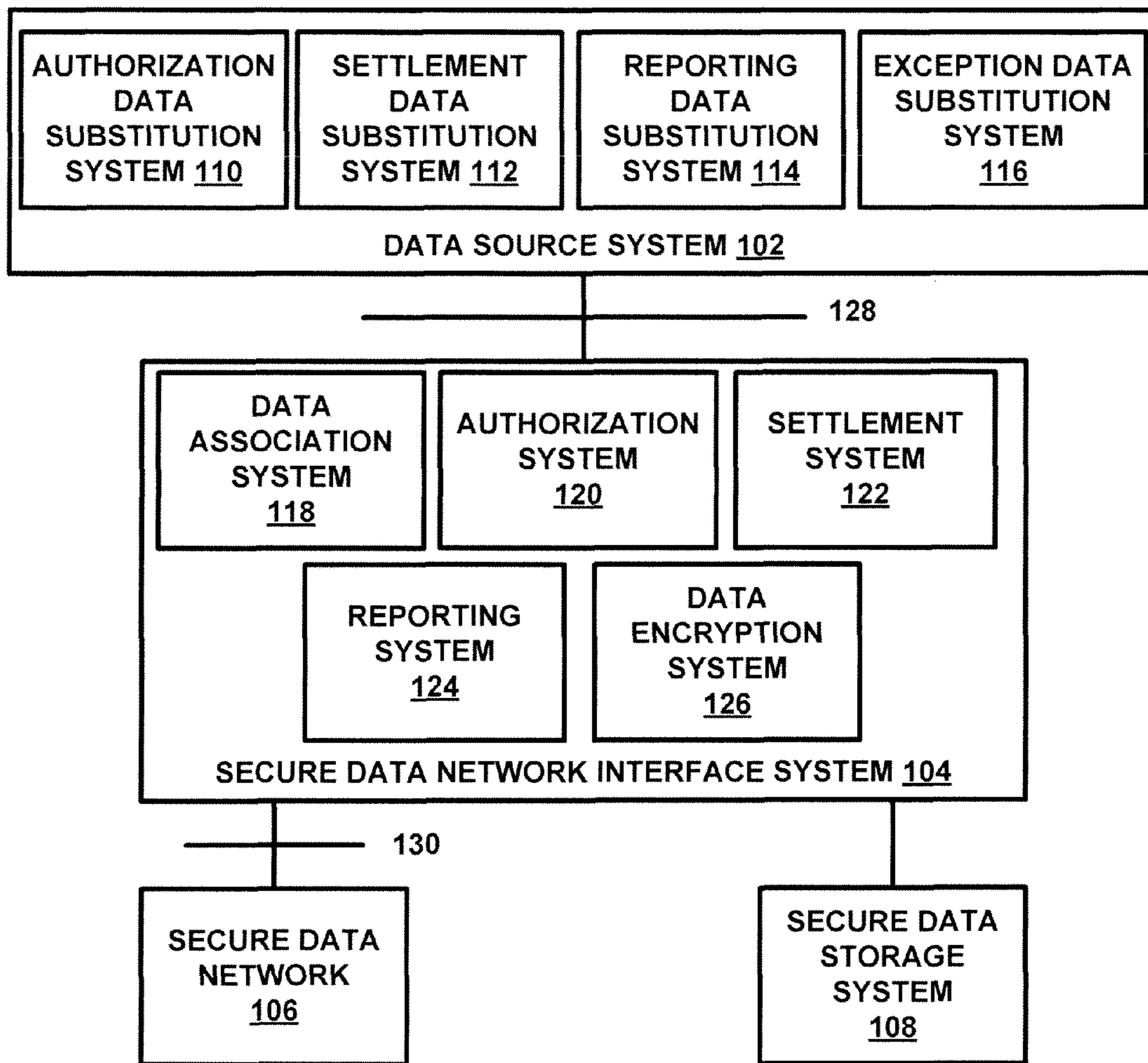
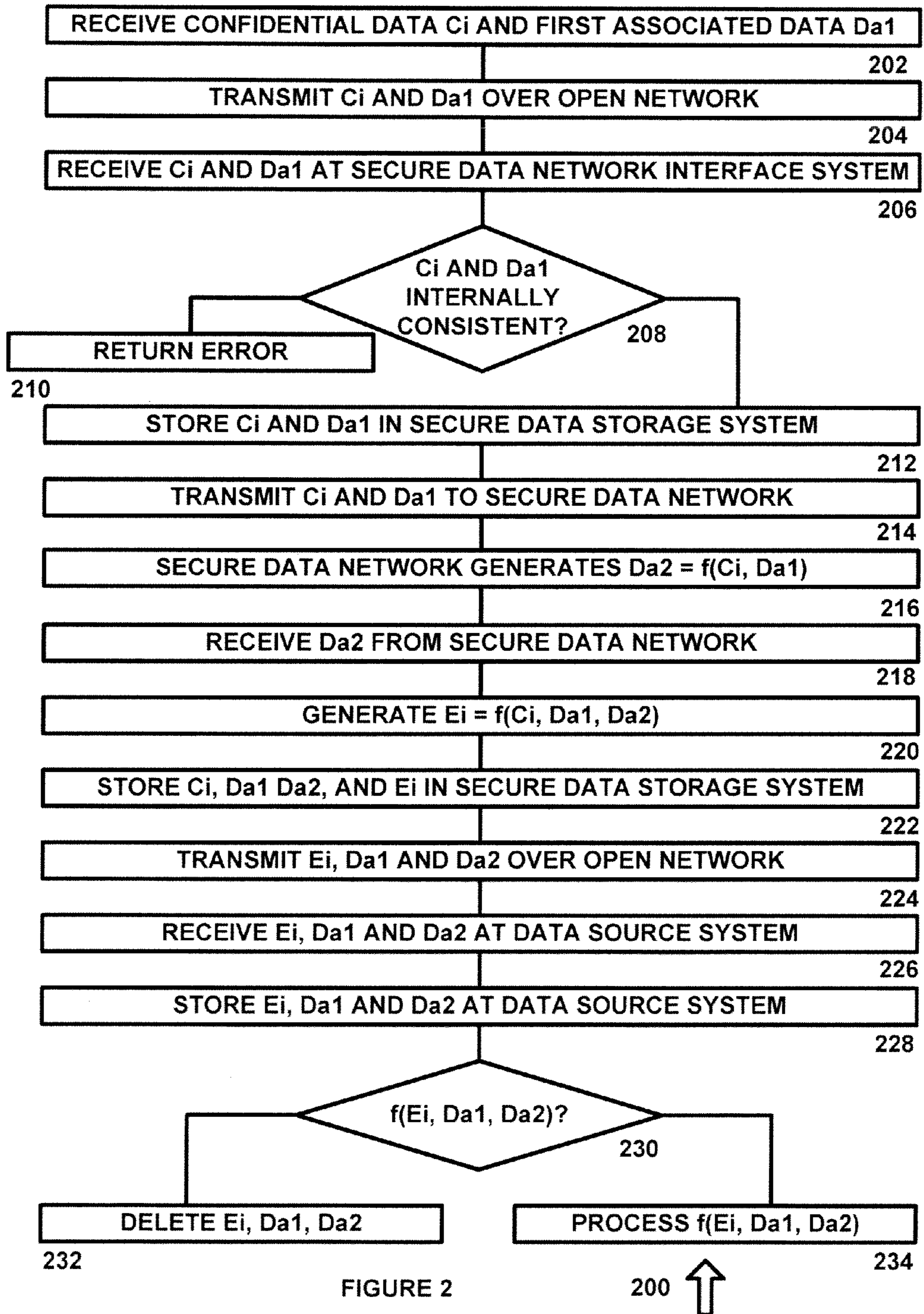


FIGURE 1

100 ↑



1

ELECTRONIC AUTHORIZATION SYSTEM AND METHOD

CROSS-REFERENCE TO RELATED APPLICATION

This application claims priority to U.S. Provisional Application No. 60/676,681, filed Apr. 29, 2005, is a continuation of U.S. Pat. No. 7,451,481, issued Nov. 11, 2008, and a divisional of U.S. Pat. No. 8,010,791, issued Aug. 30, 2011, and all of which are hereby incorporated by reference for all purposes.

FIELD OF THE INVENTION

The present invention pertains to the field of database systems, and more particularly to a database system and method for encryption and protection of confidential information that uses a unique surrogate identifier for confidential information that is stored on devices that are accessible over an open network.

BACKGROUND OF THE INVENTION

Data communications channels such as computer networks have varying degrees of security. Some computer networks, such as the Internet, are open to a large number of users. Computers that are connected to these networks may be subject to attack from third parties that want access to confidential information that is stored on the computers. This problem can be exacerbated when the confidential information is third party confidential information that is only used for short periods of time and which is then stored for future use, such as personnel data, medical data, business data, financial data, or other data.

Although firewalls and other security devices can be used to provide some protection, active monitoring of network state and data flows is required to provide the highest level of security. However, most businesses cannot afford to provide such high levels of security.

SUMMARY OF THE INVENTION

In accordance with the present invention, an electronic authorization system is provided that overcomes known problems with encryption and protection of confidential data.

In particular, an electronic authorization system is provided that does not require confidential data to be stored in a manner where it is accessible over an open network.

In accordance with an exemplary embodiment of the present invention, an electronic authorization system comprising a data source system configured to transmit transaction data. A secure data system is coupled to the data source system over an open network, the secure data system is configured to receive the transaction data from the data source system, generate a unique encrypted identifier for the transaction data and to transmit the unique encrypted identifier to the data source system. The data source system is configured to receive the unique encrypted identifier and replace payment card data associated with the transaction data in a database with the unique encrypted identifier.

The present invention provides many important technical advantages. One important technical advantage of the present invention is a system and method for managing merchant payment transaction processing accounts that allows a user to obtain pricing information without giving the user access to

2

proprietary information, such as tiered pricing structures that are developed using knowledge that has been accumulated for classes of merchants.

Those skilled in the art will further appreciate the advantages and superior features of the invention together with other important aspects thereof on reading the detailed description that follows in conjunction with the drawings.

BRIEF DESCRIPTION OF THE DRAWINGS

FIG. 1 is a diagram of a database system for encryption and protection of confidential data in accordance with an exemplary embodiment of the present invention; and

FIG. 2 is a flow chart of a method for encryption and protection of confidential data.

DETAILED DESCRIPTION OF PREFERRED EMBODIMENTS

In the description that follows, like parts are marked throughout the specification and drawings with the same reference numerals, respectively. The drawing figures might not be to scale, and certain components can be shown in generalized or schematic form and identified by commercial designations in the interest of clarity and conciseness.

FIG. 1 is a diagram of a database system **100** for encryption and protection of confidential data in accordance with an exemplary embodiment of the present invention. System **100** allows a computer on an open network to perform functions with confidential information without requiring that computer to store the confidential information so as to protect the confidential information from misappropriation.

Database system **100** includes data source system **102**, secure data network interface system **104**, secure data network **106** and secure data storage system **108**, each of which can be implemented in hardware, software, or a suitable combination of hardware and software, and which can be one more software systems operating on a suitable processing platform. As used herein, a hardware system can include a suitable general purpose processor, an application specific integrated circuit, a field programmable gate array, or other suitable systems. A software system can include one or more objects, agents, threads, lines of code, subroutines, separate software applications, two or more lines of code or other suitable software structures operating in two or more software applications or on two or more processors, or other suitable software structures. In one exemplary embodiment, a software system can include one or more lines of code or other suitable software structures operating in a general purpose software application, such as an operating system, and one or more lines of code or other suitable software structures operating in a specific purpose software application.

Data source system **102** receives confidential data C_i and first associated data Da_1 . Confidential data C_i can be confidential business data, personal data, financial data, technical data, or other suitable data. First associated data Da_1 can be non-confidential data that is associated with the confidential data, such as a file structure that has had all confidential data removed, a record identifier, a transaction identifier, or other suitable data. Confidential data C_i and first associated data Da_1 is then provided to secure data network **106** through secure data network interface system **104**, and first associated data Da_1 , unique encrypted identifier E_1 , second associated data Da_2 without confidential data C_i is received in response. Data source system **102** stores first associated data Da_1 , unique encrypted identifier E_1 , second associated data Da_2 without confidential data C_i , so as to prevent unwanted access

to confidential data C_i at data source system **102** over open network **128**. In one exemplary embodiment, data source system **102** stores the unique encrypted identifier E_i until a predetermined period of time has elapsed.

In another exemplary embodiment, data source system **102** requests additional data DaN from secure data network **106** through secure data network interface system **104** using the unique encrypted identifier E_i , and secure data network interface system **104** translates unique encrypted identifier E_i to confidential information C_i for transmission over secure data network **106**. This request can be made by sending a structured request that contains only that information, a sequence of messages with that information, fields within an existing data format (such as the VISAD data format with that information, encrypted or unencrypted, or in other suitable manners. In one exemplary embodiment, secure data network interface system **104** translates confidential information C_i using unique encrypted identifier E_i to transmit the additional data DaN to data source system **102** over open network **128**. In this exemplary embodiment, data fields in a pre-existing or proprietary data format that are blank, filler fields, or unassigned can be used to indicate that the message contains a request to translate E_i to C_i , so as to allow systems that are configured to process the pre-existing or proprietary data formats to also process the translation requests. Data source system **102** can also store the unique encrypted identifier E_i until a predetermined period of time has elapsed, until a predetermined period of time has elapsed after additional data DaN is received from secure data network **108**.

Settlement data substitution system **112** transmits a settlement request S_r and unique encrypted identifier E_i to secure data network interface system **104** and receiving a settlement confirmation S_c and unique encrypted identifier E_i from secure data network interface system **104**. This request can be made by sending a structured request that contains only that information, a sequence of messages with that information, fields within an existing data format (such as the VISAD data format or a proprietary data format) with that information, encrypted or unencrypted, or in other suitable manners. Data fields in a pre-existing or proprietary data format that are blank, filler fields, or unassigned can be used to indicate that the message contains S_r and E_i or to receive S_c and E_i , so as to allow systems that are configured to process the pre-existing or proprietary data formats to also process the settlement requests.

Reporting data substitution system **114** allows reporting data to be generated using unique encrypted identifier E_i . In one exemplary embodiment, data source system **102** provide unique encrypted identifier E_i to secure data network interface system **104** with report request R_r , and secure data network interface system **104** and secure data network **106** generate a report based on unique encrypted identifier E_i and report request R_r . This request can be made by sending a structured request that contains only that information, a sequence of messages with that information, fields within an existing data format (such as the VISAD data format or a proprietary data format) with that information, encrypted or unencrypted, or in other suitable manners. Data fields in a pre-existing or proprietary data format that are blank, filler fields, or unassigned can be used to indicate that the message contains R_r and E_i or to receive the report, so as to allow systems that are configured to process the pre-existing or proprietary data formats to also process the settlement requests.

Exception data substitution system **116** receives exception data D_d and unique encrypted identifier E_i from secure data network interface system **104** and transmits exception

response data D_r to secure data network interface system **104** in response to exception data D_d . Exception data substitution system **116** receives a transaction identifier T_i , exception category data D_c and the unique encrypted identifier E_i from secure data network interface system **104** and transmits biometric data B_d to secure data network interface system **104** in response to the transaction identifier T_i , the exception category data D_c and the unique encrypted identifier E_i . This request can be made by sending a structured request that contains only that information, a sequence of messages with that information, fields within an existing data format (such as the VISAD data format or a proprietary data format) with that information, encrypted or unencrypted, or in other suitable manners. Data fields in a pre-existing or proprietary data format that are blank, filler fields, or unassigned can be used to indicate that the message contains D_r or B_d and to receive D_c , so as to allow systems that are configured to process the pre-existing or proprietary data formats to also process the settlement requests.

Secure data network interface system **104** receives confidential data C_i and first associated data $Da1$ from data source system **102**, stores confidential data C_i and first associated data $Da1$ in secure data storage system **108**, and interfaces with systems over secure data network **106** to obtain second associated data $Da2$. In one exemplary embodiment, secure data network interface system **104** can access frame relay connections, dedicated communications lines, or other secure data communications media to obtain second associated data $Da2$ in response to the confidential data C_i and first associated data $Da1$, additional data DaN in response to subsequent queries, or other suitable data. Secure data network interface system **104** provides unique encrypted identifier E_i and second associated data $Da2$ to data source system **102** over open network **128**.

Secure data network interface system **104** includes data association system **118**, authorization system **120**, settlement system **122**, reporting system **124** and data encryption system, each of which can be implemented in hardware, software or a suitable combination of hardware and software, and which can be one or more software systems operating on a general purpose processing platform. Secure data network interface system **104** can receive a structured request that only contains information from one or more systems of data source system **102**, a sequence of messages with that information, fields within an existing data format (such as the VISAD data format or a proprietary data format) with that information, encrypted or unencrypted, or in other suitable manners. Data fields in a pre-existing or proprietary data format that are blank, filler fields, unassigned can be used to indicate that the message contains data from one or more of the systems of data source system **102**, or to transmit data to those systems, so as to allow systems that are configured to process the pre-existing or proprietary data formats to also process the settlement requests.

Data association system **118** associates the confidential data C_i with unique encrypted identifier E_i and stores confidential data $E1$, first associated data $Da1$ and unique encrypted identifier E_i in secure data storage system **108**. In one exemplary embodiment, unique encrypted identifier E_i can be keyed to some or all of the data in first associated data $Da1$, confidential data C_i , both E_i and C_i , state data that indicates whether data has been received from data source system **102**, secure data network **106**, or other suitable sources, or other suitable data. Data association system **118** also receives second associated data $Da2$, associates second associated data $Da2$ with confidential data C_i , first associated data $Da1$ and unique encrypted identifier E_i , and stores con-

5

confidential data C_i , first associated data $Da1$ and unique encrypted identifier E_i in secure data storage system **108**.

Authorization system **120** performs authorization using the confidential information C_i and the first associated data $Da1$. In one exemplary embodiment, authorization system **120** can send an authorization request Ar to secure data network **106**, and can receive an authorization indicator A_i that identifies whether authorization was approved or denied, the reason why authorization was denied, a request for additional information, or other suitable data.

Settlement system **122** performs settlement using the confidential information C_i and the first associated data $Da1$. In one exemplary embodiment, settlement system **122** can send a settlement request Sr to secure data network **106**, and can receive settlement data Sd that identifies whether settlement was processed or denied, the reason why settlement was denied, a request for additional information, or other suitable data.

Reporting system **124** provides reporting functions using unique encrypted identifier E_i , confidential data C_i , first associated data $Da1$, second associated data $Da2$, additional data DaN , or other suitable data. In one exemplary embodiment, reporting system **124** can receive plurality of unique encrypted identifiers and can obtain the corresponding confidential data C_i , first associated data second associated data $Da2$, authorization request Ar , authorization indicator A_i , settlement request Sr , settlement data Sd , or other suitable data, and can generate reports based on the types of data specified, available data, or other suitable data.

Data encryption system **126** generates a unique encrypted identifier E_i for confidential data C_i . In one exemplary embodiment, the unique encrypted identifier E_i can have the same data format as the confidential information, so as to allow the data source system to operate without modification. In this exemplary embodiment, the data source system can store the unique encrypted identifier E_i as if it were the unencrypted confidential information, so as to allow the use of the unique encrypted identifier E_i to be seamlessly transparent to the user of data source system **102**. Likewise, suitable systems can be used to interface with existing systems of data source system **102** so as to locally translate the unique encrypted identifier E_i , to modify the systems of data source system **102** to accept a unique encrypted identifier E_i that has a different size or data structure than the confidential data C_i , or to perform other suitable functions.

Secure data storage system **108** is coupled to secure data network interface system **104**, and is isolated from open network **128**. In one exemplary embodiment, secure data storage system **108** can be isolated from secure data network interface system **104** by a dedicated communications medium, one or more firewalls, and can have other suitable security measures, such as active monitoring for security threats. As such, the level of security that can be provided using secure data storage system **108** is much greater than is typically provided for data source system **102**.

Secure data network **106** is coupled to secure data network interface system **104**, receives the confidential data C_i and the first associated data $Da1$, and generates second associated data $Da2$. Secure data network **106** provides second associated data $Da2$ to secure data network interface system **104**.

In operation, database system **100** allows confidential information C_i to be used over an open network without the need to store the confidential information in a data storage device that is accessible over the open network. In this manner, data source systems can receive confidential medical data, financial data, personal data, or other suitable data and can perform a variety of functions using the confidential data

6

without the need to store the confidential data or otherwise incur costs for protecting the confidential data from third parties.

FIG. 2 is a flow chart of a method **200** for encryption and protection of confidential data. Method **200** begins at **202** where confidential data C_i and first associated data $Da1$ is received, such as at a data source system. The method then proceeds to **204** where the confidential data C_i and the first associated data $Da1$ is transmitted from the data source system over an open network to a data network interface system. The method then proceeds to **206**.

At **206**, confidential data C_i and first associated data $Da1$ is received at a secure data network interface system, and it is determined at **208** whether C_i and $Da1$ are internally consistent. In one exemplary embodiment, confidential data C_i and first associated data $Da1$ can have a predetermined structure with alpha and numeric fields, predetermined field values, address data, or other suitable data, and it can be determined whether the data is internally consistent. If the data is not internally consistent, the method proceeds to **210** and an error is returned. Otherwise, the method proceeds to **212** where C_i and $Da1$ are stored in a secure data storage system that is coupled to the data network interface system and isolated from the open network. The method then proceeds to **214**.

At **214**, confidential data C_i and first associated data $Da1$ is transmitted to a secure data network. At **216**, second associated data $Da2$ is generated at the secure data network in response to confidential data C_i and first associated data $Da1$. In exemplary embodiments, second associated data $Da2$ can be medical claim data, financial data, credit card authorization data, funds transfer data, national security data, crime enforcement data, or other suitable data. The method then proceeds to **218** where the second associated data $Da2$ is received from the secure data network at the secure data network interface system. At **220**, unique encrypted identifier E_i is generated, such as based on confidential data C_i , first associated data $Da1$ and second associated data $Da2$, or other suitable data. In exemplary embodiments, the format of the unique encrypted identifier E_i can be the same as the format of the confidential data C_i , the content of the data fields of E_i can be generated from the content of $Da1$ and $Da2$, or other suitable processes can be used. The method then proceeds to **222**.

At **222**, second associated data $Da2$ is associated with the confidential data C_i , the first associated data $Da1$, and the unique encrypted identifier E_i at the secure data network interface system. The confidential data C_i , first associated data $Da1$, second associated data $Da2$, and the unique encrypted identifier E_i can be stored in the secure data storage system. The method then proceeds to **224**.

At **224**, unique encrypted identifier E_i and second associated data $Da2$ is transmitted to the data source system over the open network, and E_i , $Da1$, $Da2$ and other suitable data is stored at the data source system, without the confidential data, so as to prevent unwanted access to the confidential data at the data source system over the open network. The method then proceeds to **230**.

At **230**, it is determined whether additional data has been requested from the secure data network through the secure data network interface system using the unique encrypted identifier E_i . If it is determined that a predetermined period of time has elapsed since the unique encrypted identifier E_i has been received without a suitable function being implemented, then the method proceeds to **232** where the data is deleted. Otherwise, a suitable function is performed. For example, unique encrypted identifier E_i and other suitable data can be transmitted to the secure data network interface system for

transmission over the secure data network, the confidential information can be translated to the unique identifier to transmit the additional data to the data source system over the open network. A settlement request can be transmitted with the unique identifier to the secure data network interface system, and a settlement confirmation and the unique identifier can be received from the secure data network interface system. Exception data and unique encrypted identifier can also be received from the secure data network interface system and exception response data can be transmitted to the secure data network interface system in response to the exception data. A transaction identifier, exception category data and the unique identifier can also be received from the secure data network interface system and biometric data can be transmitted to the secure data network interface system in response to the transaction identifier, the exception category data and the unique identifier.

Although exemplary embodiments of a system and method of the present invention have been described in detail herein, those skilled in the art will also recognize that various substitutions and modifications can be made to the systems and methods without departing from the scope and spirit of the appended claims.

What is claimed is:

1. An electronic authorization system comprising:
 - a data source system operating on a first processor and configured to transmit transaction data;
 - a secure data system operating on a second processor and coupled to the data source system over an open network, the secure data system is configured to receive the transaction data from the data source system, generate a unique encrypted identifier for the transaction data and to transmit the unique encrypted identifier to the data source system;
 wherein the data source system is configured to receive the unique encrypted identifier and replace payment card data associated with the transaction data in a database with the unique encrypted identifier.
2. The system of claim 1 wherein the data source system is configured to store the unique encrypted identifier until a predetermined period of time has elapsed after settlement data is received from the secure data network.
3. The system of claim 1 wherein the data source system is configured to transmit a settlement request and the unique encrypted identifier to the secure data system and to receive a settlement confirmation and the unique encrypted identifier from the secure data system.
4. The system of claim 1 wherein the data source system is configured to receive exception data and the unique identifier from the secure data system and to transmit exception response data to the secure data system in response to the exception data.
5. The system of claim 1 wherein the data source system is configured to receive a transaction identifier, exception category data and the unique identifier from the secure data system and to transmit biometric data to the secure data system in response to the transaction identifier, the exception category data and the unique identifier.
6. The system of claim 1 wherein the data source system and the secure data network interface system are configured to utilize spare data fields in a standardized messaging format to communicate using the unique encrypted identifier.
7. The system of claim 1, further comprising:
 - the data source system configured to transmit unique transaction data identifying a unique transaction; and
 - the secure data system configured to receive the unique transaction data from the data source system, generate

the unique encrypted identifier for the unique transaction data and to transmit the unique encrypted identifier to the data source system.

8. The system of claim 1 wherein the data source system comprises a merchant transaction system and the transaction data comprises payment card data and transaction data that identifies a unique transaction between the merchant transaction system and a payment card owner.

9. The system of claim 1 wherein the data source system comprises a merchant transaction system configured to receive the payment card data and to store the payment card data in the database at the merchant transaction system, and the transaction data comprises the payment card data and transaction data that identifies a unique transaction between the merchant transaction system and a payment card owner.

10. A method for electronic authorization comprising:

- receiving transaction data from a data source system over an open network at a secure data network;
- generating a unique encrypted identifier for the transaction data at the secure data network using a processor;
- storing the transaction data and the unique encrypted identifier at the secure data network in a non-volatile memory device; and
- transmitting the unique encrypted identifier to the data source system in a message format that causes the data source system to replace stored payment card data with the unique encrypted identifier.

11. The method of claim 10 further comprising storing the unique encrypted identifier at the data source system until a predetermined period of time has elapsed after additional data is received from the secure data network.

12. The method of claim 10 further comprising transmitting a settlement request and the unique encrypted identifier to the secure data network and receiving a settlement confirmation and the unique encrypted identifier from the secure data network.

13. The method of claim 10 further comprising receiving exception data and the unique encrypted identifier from the secure data network and transmitting exception response data to the secure data network in response to the exception data.

14. The method of claim 10 further comprising receiving a transaction identifier, exception category data and the unique encrypted identifier from the secure data network and transmitting biometric data to the secure data network in response to the transaction identifier, the exception category data and the unique identifier.

15. The method of claim 10 further comprising storing the unique encrypted identifier in non-message payload fields in a messaging format to communicate using the unique encrypted identifier.

16. The method of claim 10 wherein receiving the transaction data from the data source system over the open network at the secure data network comprises receiving unique transaction data from the data source system over the open network at the secure data network that identifies a unique transaction.

17. The method of claim 16 wherein generating the unique encrypted identifier for the transaction data at the secure data network comprises generating the unique encrypted identifier for the unique transaction data at the secure data network.

18. The method of claim 10 wherein receiving transaction data from the data source system over the open network at the secure data network comprises receiving the payment card data and unique transaction data that identifies a unique transaction over the open network at the secure data network.

19. The method of claim 10 wherein receiving transaction data from the data source system over the open network at the

secure data network comprises receiving the payment card data and unique transaction data that identifies a unique transaction over the open network at the secure data network in an encrypted format.

5

* * * * *